IT Professional Technical Services
Master Contract Program
T#:902TS

Statement of Work (SOW)
For Technology Services
Issued By

Minnesota Department of
Employment & Economic Development

Project Title: Firewall Interface Install & Implementation, Virtual F5 Implementation

Service Categories: Architecture Planning & Assessment - Technical, *or* Network (Data, Video, Voice) - LAN/ WAN Internet Support, *or* Network (Data, Video, Voice) – Security

Process Schedule

•	Post SOW	Thursday, January 19, 2012
•	Deadline for Questions	Wednesday, January 25, 2012 by noon Central
•	Anticipated Q&A posted	Thursday, January 26, 2012
•	**Proposals due**	**Monday, January 30, 2012 by 3:00 pm Central**
		Proposals cannot be accepted after this date/time
•	*Anticipated* vendor selection	Thursday, February 2, 2012

Business Need

It is the on-going commitment of the Department of Employment & Economic Development and the Unemployment Insurance Division (UI) to provide UI technology solutions to employers and UI applicants with the expectation of 7x24x365 availability. To meet this demand, DEED is building a new Disaster Recovery environment utilizing virtual machine technology and a unified network fabric. Vendor expertise is needed to assist with the **installation of Checkpoint Firewall interfaces** (10GbE SR Fiber, multi-mode, 2 ports) and to **virtualize the F5 Load balancers** in the environment.

Project Overview & Deliverables

Check Point Firewalls

Current environment has two Check Point Power-1 Clusters (5070 Active\Passive). They are located in separate logical datacenters but same physical location. An IPsec VPN tunnel connects both locations. We have two main regions of support, Acceptance and Production. Acceptance is located in the Enterprise side (Datacenter1) and Production (Datacenter2) is located in the Unemployment Insurance side.

Physical Environment:
- Enterprise – Active\Passive cluster Check Point 5070
  Supported Regions - UI Acceptance & Enterprise
- Unemployment Insurance – Active\Passive cluster Check Point 5070

Supported Regions - UI Production

The future environment, for which vendor help is being solicited, will implement a Long Distance vMotion solution for UI Acceptance and UI Production. Solution will include stretched layer 2 subnet virtualized with OTV across datacenters utilizing Cisco Nexus 7000. EMC VPLEX will be the shared storage solution. Cisco Global Site Selector (GSS) will be used for failover between datacenters.

Vendor deliverables for firewalls:
1. Assist/verify the Check Point architecture design
2. Assist/direct the implementation design, installation, and testing.
3. Add new Check Point cluster (Model 5070) for the LDVM to be used for UI (will reside in the Enterprise side (Datacenter1) but used only for LDVM).
4. Add 10GbE SR Fiber card (2-port) to the UI firewalls and support (4 Cards).
5. Trunk\Port Channel VLANS to the 10 GbE interface but for SYNC and External. Keep IPsec tunnel between Enterprise and UI. Enterprise will be moved at a later date, but the move is not part of this project.

F5 Load Balancers
Current environment has 6 Clusters of BIG-IP LTM 1600 Active\Standby. They are located in separate logical datacenters but same physical location. 3 BIG-IP Clusters support UI Acceptance in the Enterprise environment and 3 BIG-IP Clusters support UI Production in the UI environment. Each BIG-IP Cluster supports an isolated environment.

Physical Environment:
- **Production** - 3 Active\Standby Clusters Big-IP LTM 1600

  Supported Environments - Unemployment Insurance, Telephony@Work, FileNet

- **Acceptance** - 3 Active\Standby Clusters Big-IP LTM 1600

  Supported Environments- Unemployment Insurance, Telephony@Work, FileNet

The future environment, for which vendor help is being solicited, will implement a Long Distance vMotion solution for UI Acceptance and UI Production.

Vendor deliverable for load balancers:
1. Assist/verify the BIG-IP architecture design.
2. Assist/direct the implementation design, installation, and testing.
3. Install/implement BIG-IP Virtual Edition 4, each with support.
4. Combine BIG-IP Cluster Telephony@Work and FileNet to one BIG-IP Virtual Edition for each environment, SSL not required. Keep Unemployment Insurance BIG-IP Cluster physical for both environments, SSL required.

> *The attached 4 slide Visio document shows the current state environment for firewalls and load balancers, and the anticipated future state.*

Project Assumptions
1. Design has been completed and this project will start with a review and final approval of that design.
2. Diagrams have been generated and will be updated as part of this project.
3. Checkpoint rule base has been established and should only need minor changes as part of this project.
4. F5 load balancers will be moving from Physical to Virtual but the configuration should not change significantly as part of this project.
5. Vendor will work directly with project team as part of this project.
6. All hardware and software will be installed and ready for configuration when vendor comes on site.

Project Milestones and Schedule

Project is anticipated to start on or about **February 27, 2012.** For contract purposes, the end date of **December 28, 2012** will be used. The vendor will be expected to create a project work plan in MS Excel or MS Project with clear and specific deliverables for each task, and conduct regular meetings for consistent and timely review of project progress.

Project Environment (State Resources)

This work is a sub-project of a larger project called UI Greenfield (DR) Buildout and will use DEED resources from the main project. The DEED team has experience with Checkpoint Firewalls and F5 Load Balancers, but not with the interfaces and F5 in a virtual environment.

Staff descriptions:
   a) 2-3 DEED infrastructure / network resources will be assigned to this project based on vendor requirements / schedule
   b) It is not expected the vendor will need to provide a project manager.

Agency Project Requirements

- DEED requires the vendor to work on-site at data center #1, located at 1st National Bank Building, 332 Minnesota Street, St. Paul MN.
- Vendor will be expected to validate the design and implement the firewall interfaces and VE F5 in accordance with DEED standards, providing input on industry standards when applicable.
- Vendor must provide all documentation in an editable format approved by DEED. For instance, Microsoft Excel, Word or Visio. No documents in .pdf format will be accepted.

Responsibilities Expected of the Selected Vendor

- Vendor will be required to provide knowledge transfer to DEED staff.
- Vendor will work with DEED to develop implementation milestone dates / work plan
- A report of time spent and work completed is required at reasonable intervals during the project. This information will be used to assess project progress and validate invoice charges. Format/timing for report negotiable.

Required Skills

If the Vendor and/or resource do not have the required minimum qualifications below, they may be removed from further consideration:

1. Vendor must be certified in at least one of these Master Contract resource type(s)/ categories:
   - Architecture Planning & Assessment - Technical
   - Network (Data, Video, Voice) LAN/ WAN Internet Support
   - Network (Data, Video, Voice) - Security

   Please contact Thomas Schaeffer if you are unsure if you meet this requirement.
   Thomas.schaeffer@state.mn.us

2. Resource submitted must document **at least 3 years** of work experience certifying expert-level knowledge of Checkpoint Firewalls and F5 Load Balancers. (Describe work done that could be considered of "expert" level skill.)

Desired Skills

Points will be given based on the following desired skills/experiences of the resource submitted:

1. In order to be competitive, it is recommended the vendor should have local resources as travel & expenses will not be paid.
2. *Any work experience similar to this SOW in the private sector or the State of Minnesota. Work experience with DEED is desirable.*

Questions

Questions regarding this Statement of Work should be submitted via e-mail by the deadline noted above to:

Thomas Schaeffer, Manager of Infrastructure and Datacenter Operations
Thomas.Schaeffer@state.mn.us

Vendor will be sent an email response and all questions/answers will be sent to all vendors.

SOW Evaluation Process

Proposals will be evaluated as follows:

Overall Experience – 40%
Project Approach – 30%
Cost – 30%

Response Requirements

The proposal should be assembled as follows:

Cover Page: Vendor Name
Vendor Address
Vendor City, State, Zip
Contact Name for Vendor
Contact's direct phone
Contact's email
Resource Name being submitted

Overall Experience:

1. Provide narrative, including companies and contacts where your resource has demonstrated expert-level knowledge of Checkpoint Firewalls and F5 Load Balancers. If resource cannot demonstrate this background, the State reserves the right to discontinue further scoring of the proposal.
2. Points will also be awarded based on the **desired skills** noted above. **Provide one paragraph** which highlights the resource's desired skills noted above.
3. Attach a **resume(s) for proposed resource(s)** in addition to the narrative description. Be certain the resume has dates of work and notes whether the resource was an employee or consultant.
4. Also include the name of **ONE reference** who can speak to the resources work on a similar project. Include the company name and address, reference name, reference email, reference phone number and a brief description of the project this resource completed.

❖ *This section of Overall Experience is worth 40% of the proposals total score.*

Project Approach:

Describe the approach vendor will take to execute this work and ensuring all completion of all deliverables or additional work as deemed appropriate. Vendor should also submit a high level timeline for the work.

Remember to include any assumptions or requirements/responsibilities from/of DEED staff. Also include any best practices which would make this project successful that have not been mentioned in the deliverables. Please clearly delineate if additional work is being added to the scope so the cost may be analyzed appropriately.

❖ *This section of Project Approach is worth 30% of the proposals total score.*

Cost: **This contract will be Time and Materials.** Based on the work described in the Project Deliverables section of this Statement of Work, show in a simple chart the resource cost and time estimates for each deliverable, with a final best estimate of total cost. *Be sure and note any additional best practice work described in your Project Approach.*

❖ *This section of Cost is worth 30% of the proposals total score.*

State Forms
Include the following forms in the last section.

Required forms to be returned or additional provisions that must be included in proposal
a) Affidavit of non-collusion
   http://www.mmd.admin.state.mn.us/doc/noncollusion.doc
b) Veteran-Owned/Service Disabled Veteran-Owned Preference Form (if applicable)
   http://www.mmd.admin.state.mn.us/doc/vetpref.doc

Proposal Submission Instructions

Submit proposals **via email** with subject line **Firewall & F5 VE Proposal** to:

Thomas Schaeffer, Manager of Infrastructure and Datacenter Operations
Thomas.Schaeffer@state.mn.us

A reply will be sent confirming receipt of the proposal.
Proposals must be received before date/time noted in the Process Schedule section above.

General Requirements

Proposal Contents
By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of this work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Liability
In the performance of this contract by Contractor, or Contractor's agents or employees, the contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:
   1) Intentional, willful, or negligent acts or omissions; or
   2) Actions that give rise to strict liability; or
   3) Breach of contract or warranty.
The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

Disposition of Responses
All materials submitted in response to this SOW will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this RFP, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.

Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor's objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage. The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration's Materials Management Division ("MMD") which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve the State's rights.

IT Accessibility Standards

Responses to this solicitation must comply with the Minnesota IT Accessibility Standards effective September 1, 2010, which entails, in part, the Web Content Accessibility Guidelines (WCAG) 2.0 (Level AA) and Section 508 Subparts A-D which can be viewed at: **http://www.mmd.admin.state.mn.us/pdf/accessibility_standard.pdf**

Nonvisual Access Standards

Nonvisual access standards require:

1) The effective interactive control and use of the technology, including the operating system, applications programs, prompts, and format of the data presented, are readily achievable by nonvisual means;
2) That the nonvisual access technology must be compatible with information technology used by other individuals with whom the blind or visually impaired individual must interact;
3) That nonvisual access technology must be integrated into networks used to share communications among employees, program participants, and the public; and
4) That the nonvisual access technology must have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Veteran-owned/Service Disabled Veteran-Owned Preference

In accordance with Minnesota Statute §16C.16, subd. 6a, veteran-owned businesses with their principal place of business in Minnesota and verified as eligible by the United States Department of Veterans Affairs' Center for Veteran Enterprises (CVE Verified) will receive up to a 6 percent preference in the evaluation of its proposal.

Eligible veteran-owned small businesses include CVE verified small businesses that are majority-owned and operated by either recently separated veterans, veterans with service-connected disabilities, and any other veteran-owned small businesses (pursuant to Minnesota Statute §16C.16, subd. 6a).

Information regarding CVE verification may be found at http://www.vetbiz.gov.

Eligible veteran-owned small businesses should complete and **sign** the **Veteran-Owned Preference Form** in this solicitation. Only eligible, CVE verified, veteran-owned small businesses that provide the required documentation, per the form, will be given the preference.

Foreign Outsourcing of Work Prohibited

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.
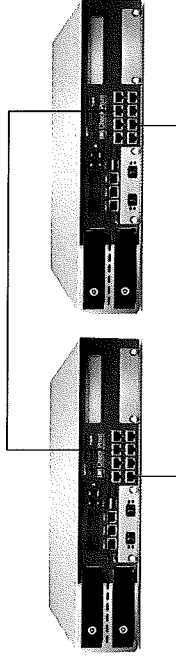
Current Firewall Logical Diagram
First National Bank

Checkpoint Firewalls
DR – Active\Passive
Datacenter2
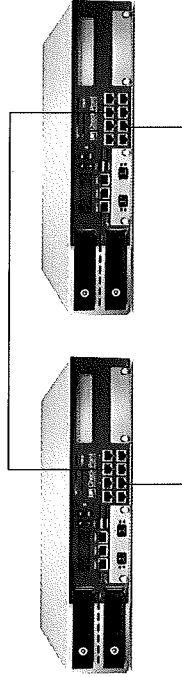
Checkpoint Firewalls
FNB – Active\Passive
Datacenter1

Ipsec VPN Tunnel
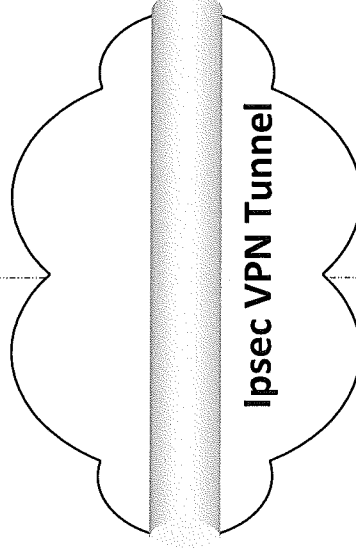
Future Firewall Logical Diagram
Long Distance vMotion
First National Bank

MNET

Cisco GSS

Cisco GSS

Checkpoint Firewalls
DR – Active\Passive
Datacenter2

Checkpoint Firewalls
FNB – Active\Passive
Datacenter1
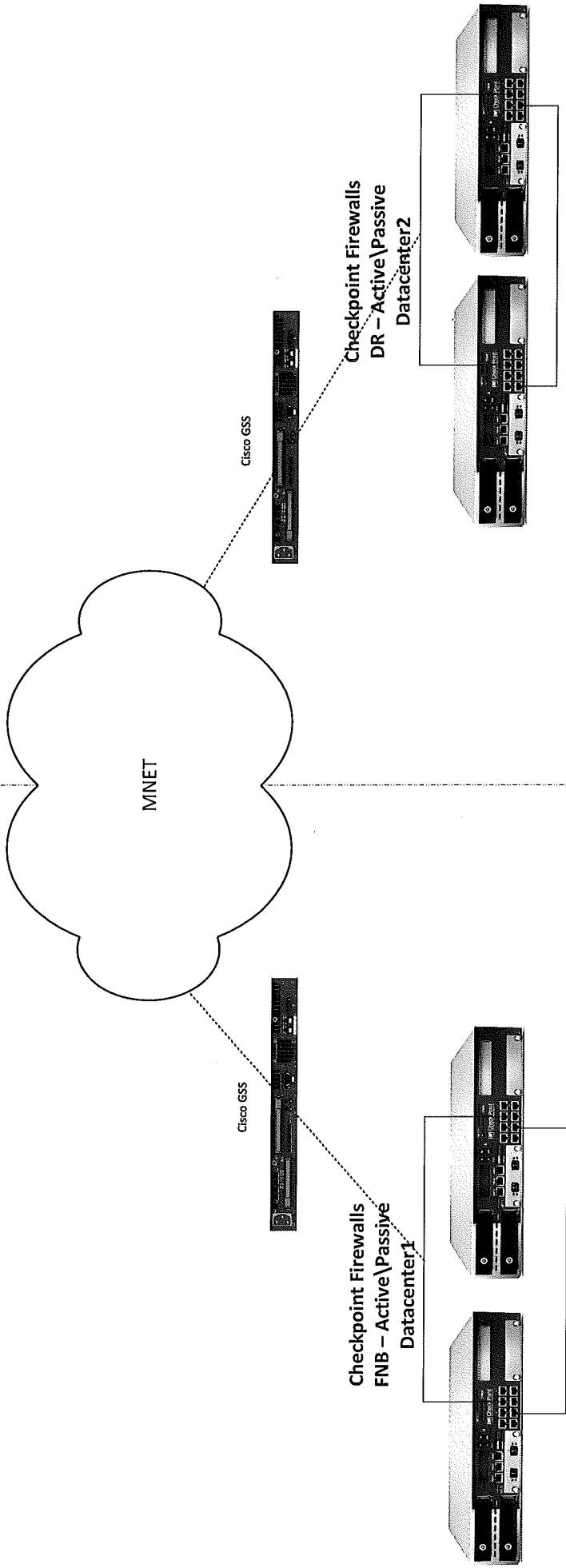
VIP Logical Diagram
Each Firewall Interface needs Physical Layer 3 Connection

Current F5 Logical Diagram
First National Bank

Checkpoint Firewalls
DR – Active\Passive

VIP to Internal

Cisco Core

FileNet

TAW

UI

Physical Production F5 LTM Load Balancers

Ipsec VPN Tunnel

Checkpoint Firewalls
FNB – Active\Passive

VIP to Internal

Cisco Core

FileNet

TAW

UI

Physical Acceptance F5 LTM Load Balancers

Checkpoint Firewalls
DR – Active\Passive

Cisco GSS

Cisco Nexus 7010

VMWare Server Farm

MNET

Cisco GSS

Checkpoint Firewalls
FNB – Active\Passive

Cisco Nexus 7010

OTV Long Distance vMotion
Stretched Layer 2 Subnet

Production Physical
UI

Acceptance Physical
UI

VMWare Server Farm

Production Physical
UI

Acceptance Physical
UI

VM TAW Virtual Edition   VM FileNet Virtual Edition
Production   Production

VM TAW Virtual Edition   VM FileNet Virtual Edition
Acceptance   Acceptance